Chapter 4 Resource

Network Security

Chapter Summary

In this chapter, we covered computer networking and securing the network. A network is simply two or more computers linked together to share data, information or resources. There are many types of networks, such as LAN, WAN, WLAN and VPN, to name a few. Some of the devices found on a network can be hubs, switches, routers, firewalls, servers, endpoints (e.g., desktop computer, laptop, tablet, mobile phone, VOIP or any other end-user device). Other network terms you need to know and understand include ports, protocols, ethernet, Wi-Fi, IP address and MAC address.

The two models discussed in this chapter are OSI and TCP/IP. The OSI model has seven layers and the TCP/IP four. They both take the 1s and 0s from the physical or network interface layer, where the cables or Wi-Fi connect, to the Application Layer, where users interact with the data. The data traverses the network as packets, with headers or footers being added and removed accordingly as they get passed layer to layer. This helps route the data and ensures packets are not lost and remain together. IPv4 is slowly being phased out by IPv6 to improve security, improve quality of service and support more devices.

As mentioned, Wi-Fi has replaced many of our wired networks, and with its ease of use, it also brings security issues. Securing Wi-Fi, e.g., using WPA2, is very important.

We then learned about some of the attacks on a network, e.g., DoS/DDoS attacks, fragment attacks, oversized packet attacks, spoofing attacks, and man-in-the middle attacks. We also discussed the ports and protocols that connect the network and services that are used on networks, from physical ports, e.g., LAN port, that connect the wires, to logical ports, e.g., 80 or 443, that connect the protocols/services.

We then examined some possible threats to a network, including spoofing, DoS/DDoS, virus, worm, Trojan, on-path (man-in-the-middle) attack, and side-channel attack. The chapter went on to discuss how to identify threats, e.g., using IDS/NIDS/HIDS or SIEM, and prevent threats, e.g., using antivirus, scans, firewalls, or IPS/NIPS/HIPS. We discussed on-premises data centers and their requirements, e.g., power, HVAC, fire suppression, redundancy and MOU/MOA. We reviewed the cloud and its characteristics, to include service models: SaaS, IaaS and PaaS; and deployment models: public, private, community and hybrid. The importance of an MSP and SLA were also discussed.

Terminology for network design, to include network segmentation, e.g., microsegmentation and demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), defense in depth, zero trust and network access control, were described in great detail.

Module Names

Module 1: Understand Computer Networking

Module 2: Understand Network Threats and Attacks

Module 3: Understand Network Security Infrastructure

Chapter to Domain Mapping

Module Number	Module Title	Domains
1	Understand Computer Networking	4.1, 4.1.1, 4.1.2, 4.1.3
2	Understand Network Threats and Attacks	4.2, 4.2.1, 4.2.2, 4.2.3
3	Understand Network Security Infrastructure	4.3, 4.3.1, 4.3.2, 4.3.3

Learning Objectives

After completing this chapter, the participant will be able to:

- Explain the concepts of network security.
- Recognize common networking terms and models.
- Identify common protocols and ports and their secure counterparts.
- Identify types of network threats and attacks.
- Discuss common tools used to identify and prevent threats.
- Identify common data center terminology.
- Recognize common cloud service terminology.
- Identify secure network design terminology.
- Practice the terminology of and review network security concepts.

Chapter Takeaways

Module 1: Understand computer networking

Types of Computer Networks:

- LAN – Local Area Network
- WAN – Wide Area Network
- WLAN – Wireless Local Area Network
- VPN – Virtual Private Network
- EPN – Enterprise Private Network
- PAN – Personal Area Network
- CAN – Campus Area Network
- MAN – Metropolitan Area Network
- SAN – Storage Area Network
- SAN – System-Area Network
- POLAN – Passive Optical Local Area Network

Network Devices:

- Hubs
- Switches
- Routers
- Firewalls
- Servers
- Printers
- Fax Machines
- Gateways
- Repeaters
- Bridges
- Modems
- Access Points
- Endpoints (e.g., desktop computer, laptop, tablet, cellphone, VOIP, or any other end-user device)

Other Network Terms:

- Packet
- Port
- Protocol
- Ethernet
- Wi-Fi
- IP address
- MAC address

Network Models:

- OSI and TCP/IP

Chapter Takeaways

Module 1: Understand computer networking (continued)

IPv4 vs IPv6:

- IPv6 is a modernization of IPv4:
  - A much larger address field (support more devices)
  - Improved security
  - Improved quality of service (QoS)

Module 2: Understand network threats and attacks

Types of Network Attacks:

- DoS/DDoS
- Fragment
- Oversized Packet
- Spoofing
- Man-in-the-Middle
- Code/SQL Injection
- XSS (Cross Site Scripting)
- Privilege Escalation
- Insider Threat

Types of Network Threats:

- Spoofing
- DoS/DDoS
- Virus
- Worm
- Trojan
- On-Path (Man-in-the-Middle)
- Side-channel
- Phishing
- Rootkit
- Adware/Spyware
- Malware

Module 2: Understand network threats and attacks

Ports and Protocols:

Insecure Port	Protocol	Secure Alternative Port	Protocol
21 - FTP	File Transfer Protocol	22* - SFTP	Secure File Transfer Protocol
23 – Telnet	Telnet	22* - SSH	Secure Shell
25 – SMTP	Simple Mail Transfer Protocol	587 – SMTP	SMTP with TLS
37 – Time	Time Protocol	123 – NTP	Network Time Protocol
53 – DNS	Domain Name Service	853 - DoT	DNS over TLS (DoT)
80 – HTTP	HyperText Transfer Protocol	443 – HTTPS	HyperText Transfer Protocol (SSL/TLS)
143 - IMAP	Internet Message Access Protocol	993 – IMAP	IMAP for SSL/TLS
161/162 - SNMP	Simple Network Management Protocol	161/162 - SNMP	SNMPv3
445 – SMB	Server Message Block	2049 - NFS	Network File System
389 – LDAP	Lightweight Directory Access Protocol	636 - LDAPS	Lightweight Directory Access Protocol Secure

How we Identify Threats:

- IDS
- NIDS
- HIDS
- SIEM

How we Prevent Threats:

- Antivirus
- Scans
- Firewalls
- IPS
- NIPS
- HIPS

Module 3: Understand network security infrastructure

Requirements for a Data Center:

- Power
- HVAC
- Fire Suppression
- Redundancy
- MOU/MOA

Cloud Service Models:

- SaaS
- IaaS
- PaaS

Cloud Deployment Models:

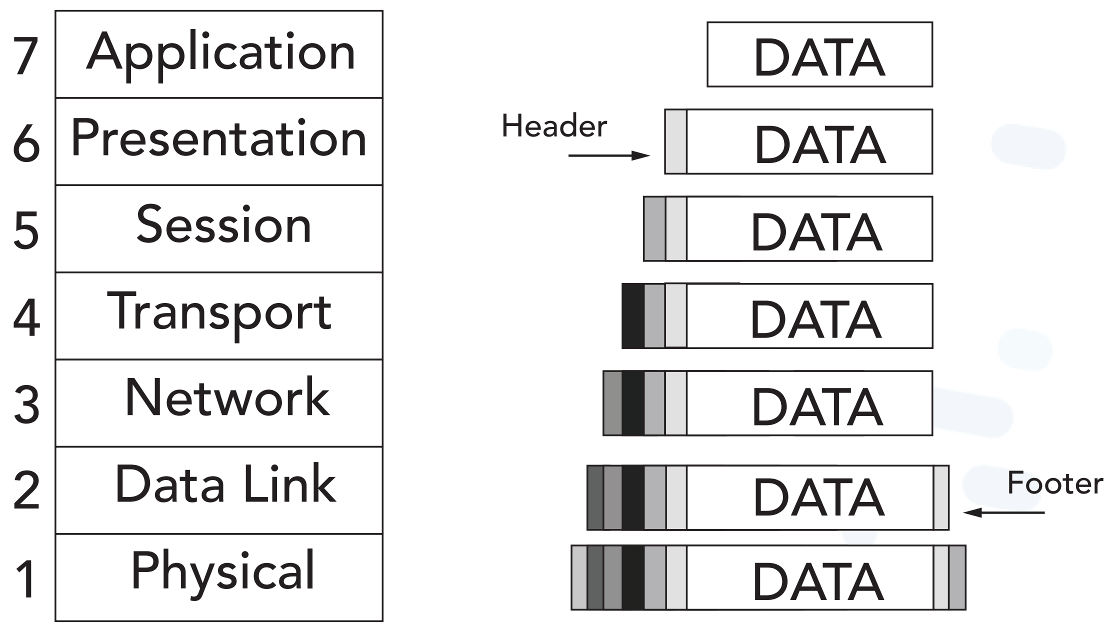
- Public
- Private
- Community
- Hybrid

Network Design Terminology:

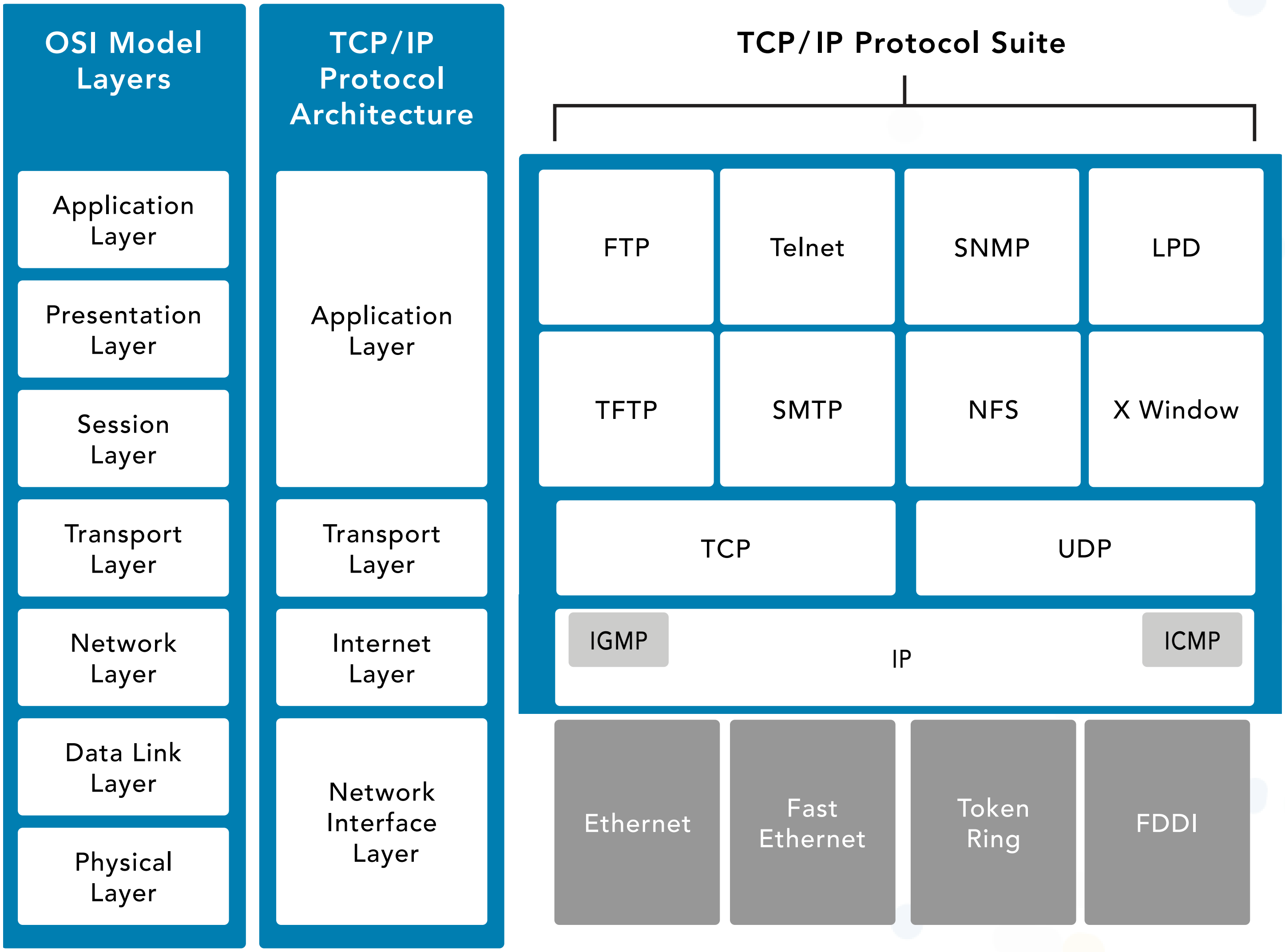
- Network Segmentation, e.g., microsegmentation and demilitarized zone (DMZ)
- Virtual Local Area Network (VLAN)
- Virtual Private Network (VPN)
- Defense in Depth
- Zero Trust
- Network Access Control

Graphics

Open Systems Interconnection (OSI) Model



Transmission Control Protocol/Internet Protocol (TCP/IP) Model



Chapter Terms and Definitions

Application programming interface (API)

A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or web tool.

Bit

The most essential representation of data (zero or one) at Layer 1 of the Open Systems Interconnection (OSI) model.

Broadcast

Broadcast transmission is a one-to-many (one-to-everyone) form of sending internet traffic.

Byte

The byte is a unit of digital information that most commonly consists of eight bits.

Cloud computing

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST 800-145

Community cloud

A system in which the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. NIST 800-145

De-encapsulation

The opposite process of encapsulation, in which bundles of data are unpacked or revealed.

Denial-of-Service (DoS)

The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) Source: NIST SP 800-27 Rev A

Domain Name Service (DNS)

This acronym can be applied to three interrelated elements: a service, a physical server and a network protocol.

Encapsulation

Enforcement of data hiding and code hiding during all phases of software development and operational use. Bundling together data and methods is the process of encapsulation; its opposite process may be called unpacking, revealing, or using other terms. Also used to refer to taking any set of data and packaging it or hiding it in another data structure, as is common in network protocols and encryption.

Encryption

The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

File Transfer Protocol (FTP)

The internet protocol (and program) used to transfer files between hosts.

Fragment attack

In a fragment attack, an attacker fragments traffic in such a way that a system is unable to put data packets back together.

Hardware

The physical parts of a computer and related devices.

Hybrid cloud

A combination of public cloud storage and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

Infrastructure as a Service (IaaS)

The provider of the core computing, storage and network hardware and software that is the foundation upon which organizations can build and then deploy applications. IaaS is popular in the data center where software and servers are purchased as a fully outsourced service and usually billed on usage and how much of the resource is used.

Internet Control Message Protocol (ICMP)

An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available.

Internet Protocol (IPv4)

Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. CNSSI 4009-2015

Man-in-the-Middle

An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them. Source: NISTIR 7711

Microsegmentation

Part of a zero-trust strategy that breaks LANs into very small, highly localized zones using firewalls or similar technologies. At the limit, this places firewall at every connection point.

Oversized Packet Attack

Purposely sending a network packet that is larger than expected or larger than can be handled by the receiving system, causing the receiving system to fail unexpectedly.

Packet

Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model.

Payload

The primary action of a malicious code attack.

Payment Card Industry Data Security Standard (PCI DSS)

Security standards that apply to merchants and service providers who process credit or debit card transactions.

Platform as a Service (PaaS)

The web-authoring or application development middleware environment that allows applications to be built in the cloud before they're deployed as SaaS assets.

Private cloud

The phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of cloud systems, but removes a number of objections to the cloud computing model, including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.

Protocols

A set of rules (formats and procedures) to implement and control some type of association (that is, communication) between systems. NIST SP 800-82 Rev. 2

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. NIST SP 800-145

Simple Mail Transport Protocol (SMTP)

The standard communication protocol for sending and receiving emails between senders and receivers.

Software

Computer programs and associated data that may be dynamically written or modified during execution. NIST SP 80--37 Rev. 2

Software as a Service (SaaS)

The cloud customer uses the cloud provider's applications running within a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Derived from NIST 800-145

Spoofing

Faking the sending address of a transmission to gain illegal entry into a secure system. CNSSI 4009-2015

Transport Control Protocol/Internet Protocol (TCP/IP) Model

Internetworking protocol model created by the IETF, which specifies four layers of functionality: Link layer (physical communications), Internet Layer (network-to-network communication), Transport Layer (basic channels for connections and connectionless exchange of data between hosts), and Application Layer, where other protocols and user applications programs make use of network services.

VLAN

A virtual local area network (VLAN) is a logical group of workstations, servers, and network devices that appear to be on the same LAN despite their geographical distribution.

VPN

A virtual private network (VPN), built on top of existing networks, that can provide a secure communications mechanism for transmission between networks.

WLAN

A wireless area network (WLAN) is a group of computers and devices that are located in the same vicinity, forming a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN.

Zenmap

The graphical user interface (GUI) for the Nmap Security Scanner, an open-source application that scans networks to determine everything that is connected as well as other information.

Zero Trust

Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Microsegmentation of workloads is a tool of the model.